DATOS BÁSICOS DE LA GUÍA DOCENTE:

Materia:	SEGURIDAD EN REDES Y SISTEMAS		
Identificador:	30552		
Titulación:	GRADUADO EN INGENIERÍA INFORMÁTICA (SEMIPRESENCIAL). 2008 (BOE 15/12/2008)		
Módulo:	COMUNICACIONES		
Tipo:	OBLIGATORIA		
Curso:	4	**Periodo lectivo:**	Segundo Cuatrimestre
Créditos:	6	**Horas totales:**	150
Actividades Presenciales:	12	**Trabajo Autónomo:**	138
Idioma Principal:	Castellano	**Idioma Secundario:**	Inglés
Profesor:		**Correo electrónico:**	

PRESENTACIÓN:

Actualmente, la Seguridad en los Sistemas de Información (SSI) a pasado de ser un área asociada a otras actividades, como desarrollo de aplicaciones, gestión de redes o administración de sistemas; a convertirse en una disciplina en sí misma. De forma análoga, cuando hace pocos años se planteaban ámbitos de estudio de la SSI, era habitual encontrar aplicaciones muy específicas relacionadas por ejemplo con criptografía y modelos matemáticos, mientras que hoy en día, términos como certificado digital, firma electrónica o protocolos seguros, han pasado de ser conceptos reservados a expertos en criptografía, a formar parte de actividades cercanas a los usuarios, gestores y responsables de sistemas de información.

Debemos valorar que los nuevos modelos sobre servicios de seguridad deben formar parte de la Sociedad de la Información y, por tanto, los profesionales involucrados en diseño de soluciones con Tecnologías de la Información (TI) deben conocer, entender y aplicar estos servicios es sus proyectos para garantizar las propiedades de la seguridad que es necesario alcanzar.

En este contexto, se pretende que la materia “Seguridad en redes y sistemas” permita al estudiante abordar los principales procesos de diseño de sistemas seguros. Incluyendo en sus contenidos aquellas técnicas, metodologías y servicios que garantizan la SSI.

COMPETENCIAS PROFESIONALES A DESARROLLAR EN LA MATERIA:

Competencias Generales de la titulación	G02	Capacidad innovadora para proponer y encontrar formas nuevas y eficaces de realizar cualquier tarea y/ o función dentro de su entorno profesional con una elevada motivación por la calidad
	G04	Capacidad para trabajar siempre con responsabilidad y compromiso, creando un alto sentido del deber y el cumplimiento de las obligaciones
	G06	Capacidad para analizar y resolver los problemas o imprevistos complejos que puedan surgir durante la actividad profesional dentro de cualquier tipo de organización socio-económica
	G10	Capacidad crítica y analítica en la evaluación de información, datos y líneas de actuación
	G12	Capacidad para desarrollar las actividades profesionales con integridad respetando normas sociales, organizacionales y éticas
	G14	Capacidad de abstracción para manejar diferentes modelos complejos de conocimiento y aplicarlos al planteamiento y resolución de problemas
Competencias Específicas de la titulación	E01	Capacidad para comprender la profesión de la ingeniería y compromiso para servir a la sociedad de acuerdo al código de conducta profesional correspondiente
	E10	Capacidad para comprender y evaluar el impacto de la tecnología en los individuos, las organizaciones, la sociedad y el medioambiente, incluyendo aspectos éticos, legales y políticos, reconociendo y aplicando los estándares y regulaciones oportunos
	E11	Capacidad para mantenerse al día en el mundo tecnológico y empresarial en el ámbito de las tecnologías de la informática y comunicaciones
	E13	Capacidad para identificar, evaluar y usar tecnologías actuales y emergentes, considerando su aplicabilidad en función de las necesidades de individuos y organizaciones
	E19	Capacidad para diseñar y definir la arquitectura de sistemas IT (software, hardware y comunicaciones) de acuerdo a unos requisitos consensuados entre las partes involucradas
Resultados de Aprendizaje	R01	Abordar aquellos procesos de diseño de sistemas seguros
	R02	Utilizar metodologías y sistemas, cuyo propósito consiste en garantizar la seguridad de la información.

	R03	Aplicar técnicas de seguridad en redes y dar soluciones en cuanto a cortafuegos, detección de intrusos, etc.
	R04	Desarrollar aplicaciones seguras frente a virus e intrusos
	R05	Entender PKI y la infraestructura de clave pública

REQUISITOS PREVIOS:

Deberán haberse cursado las siguientes asignaturas:

- Sistemas operativos
- Administración de sistemas operativos
- Administración de servidores

Se considera conveniente, pero no necesario, haber adquirido conocimientos relacionadas con criptografía en materias optativas sobre criptografía o en obligatorias sobre matemática discreta.

PROGRAMACIÓN DE LA MATERIA:

Contenidos de la materia:

1 - Visión general de la SSI
1.1 - Introducción
1.2 - Definiciones y diferentes visiones
1.3 - Propiedades y servicios de la SSI
1.4 - Seguridad en redes y SSOO
1.5 - Práctica 1: Análisis de seguridad de un caso práctico
2 - Diseño de sistema seguros
2.1 - Presentación
2.2 - Material de referencia
2.3 - Práctica 2: Despliegue de un caso práctico de PKI; PGP e IBS
3 - Ataques y virus
3.1 - Presentación
3.2 - Material de referencia
3.3 - Desarrollo y análisis de ataques
3.4 - Prácticas 3 y 4: Diseño de SSI

La planificación de la asignatura podrá verse modificada por motivos imprevistos (rendimiento del grupo, disponibilidad de recursos, modificaciones en el calendario académico, etc.) y por tanto no deberá considerarse como definitiva y cerrada.

METODOLOGÍAS Y ACTIVIDADES DE ENSEÑANZA Y APRENDIZAJE:

Metodologías de enseñanza-aprendizaje a desarrollar:

Las sesiones de prácticas no se realizan en un orden estricto. Se organizan según los temas presentados y la evolución de los trabajos propuestos. Cada tipo de sesiones, trabajo y actividades; están diseñadas para el desarrollo de las competencias que el alumno debe adquirir en la asignatura. Las recomendaciones más importantes realizadas a los alumnos se pueden resumir en el siguiente esquema:

1. Revisar las presentaciones y el material de esta unidad didáctica correspondientes a cada una de las presentaciones en sesiones presenciales antes de asistir a las sesiones presenciales (el material estará disponible en la PDU con antelación suficiente).
2. Asistencia a las sesiones de teoría de forma participativa, transmitiendo las dudas e inquietudes que hayan surgido en la revisión previa del estudiante o la durante la presentación con el profesor.
3. Complementar los temas tratados en estas sesiones con información ofrecida en cada una de

las unidades, sobre todo en las unidades “Diseño de sistema seguros” y “Ataques y virus”.

4. Utilizar, en cualquier momento, las sesiones de tutorías para resolver cualquier duda o problema

Seguir el desarrollo de las prácticas según los criterios establecidos:

- Cuando se ha explicado los conceptos teóricos necesarios y no retrasar su realización.
- Independientemente de que las actividades prácticas sean individuales o en grupo, comenzar la realización de las tareas prácticas de forma individual.
- Resolver dificultades encontradas con los compañeros de forma abierta en los foros de la materia, independientemente de que las actividades prácticas sean individuales o el grupo.

Volumen de trabajo del alumno:

Modalidad organizativa	Métodos de enseñanza	Horas estimadas
Actividades Presenciales	Clase magistral	7
	Casos prácticos	3
	Actividades de evaluación	2
Trabajo Autónomo	Asistencia a tutorías	10
	Estudio individual	20
	Preparación de trabajos individuales	25
	Preparación de trabajos en equipo	25
	Tareas de investigación y búsqueda de información	20
	Lecturas obligatorias	20
	Lectura libre	18
	Horas totales:	150

SISTEMA DE EVALUACIÓN:

Obtención de la nota final:

Trabajos individuales:	50	%
Trabajos en equipo:	50	%
TOTAL	100	%

*Las observaciones específicas sobre el sistema de evaluación serán comunicadas por escrito a los alumnos al inicio de la materia.

BIBLIOGRAFÍA Y DOCUMENTACIÓN:

Bibliografía básica:

Se facilitará toda la bibliografía necesaria en la Unidad Didáctica de la material y, en la PDU, se agregarán referencias específicas que sea necesario agregar posteriormente.

Bibliografía recomendada:

Se facilitará toda la bibliografía necesaria en la Unidad Didáctica de la material y, en la PDU, se agregarán referencias específicas que sea necesario agregar posteriormente.

Adams, C, and S Farrell. “RFC 2510 - Internet X.509 Public Key Infrastructure Certificate Management Protocols,” 1999.http:/ / tools.ietf.org/ html/ rfc2510.

Aguirre, Jorge Ramió. Libro Electrónico De Seguridad Informática y Criptografía. UPM, 2006.http:/ / www.criptored.upm.es/ guiateoria/ gt_m001a.htm.

IBM Redbooks. Implementing PKI Services on z/ OS, 2004. http:/ / www.redbooks.ibm.com/ abstracts/ SG246968.html?Open.

OpenCA Team. The Open–source PKI Book, 2000. http:/ / sourceforge.net/ projects/ ospkibook/ files/ .

PKIX Working Group. “Public-key Infrastructure (X.509) (pkix),” 2004. http:/ / www.ietf.org/ html.charters/ pkix-charter.html.

Gómez, J; Villar, E y Alcayde, A.: Seguridad en Sistemas Operativos Windows y GNU/ Linux\\; 2ª Edición,2011

Páginas web recomendadas:

Se facilitará toda la bibliografía necesaria en la Unidad Didáctica de la material y, en la PDU, se agregarán referencias específicas que sea necesario agregar posteriormente.	http://pdu.usj.es

* Guía Docente sujeta a modificaciones